R E P U B L I Q U E F R A N C A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

PCT/FR 01/01205
01/018371

REC'D 05 JUN 2001
WIPO PCT

FR01/1205

BREVET D'INVENTION

4

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 21 MAI 2001

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
http://www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES DATE 04-10-00
LIEU 99
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0013101
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI - 4 OCT. 2000

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

MAITRE BENECH
69 avenue Victor Hugo
75783 PARIS CEDEX 16

Vos références pour ce dossier *(facultatif)*

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie 2541

2 NATURE DE LA DEMANDE — **Cochez l'une des 4 cases suivantes**

Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE ET DISPOSITIF DE CERTIFICATION

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation Date / / N°
Pays ou organisation Date / / N°
Pays ou organisation Date / / N°
☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR — ☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**

Nom ou dénomination sociale		MAGICAXESS
Prénoms		
Forme juridique		SA
N° SIREN		421 516 980 00016
Code APE-NAF		722Z
Adresse	Rue	28 RUE JEAN JAURES
	Code postal et ville	92800 PUTEAUX
Pays		FRANCE
Nationalité		FRANÇAISE
N° de téléphone *(facultatif)*		01 41 97 83 53
N° de télécopie *(facultatif)*		01 41 97 83 67
Adresse électronique *(facultatif)*		gilles.bremer@wanadoo.fr

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES DATE 04-10-00

LIEU 99

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0013101

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		
6 **MANDATAIRE**		
Nom		BENECH
Prénom		FREDERIC
Cabinet ou Société		CABINET BENECH
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	69 Avenue VICTOR HUGO
	Code postal et ville	75783 PARIS CEDEX 16
N° de téléphone *(facultatif)*		0144 17 36 60
N° de télécopie *(facultatif)*		01 40 67 91 40
Adresse électronique *(facultatif)*		benech2 benech.com
7 **INVENTEUR (S)**		GILLES KREMER
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 **RAPPORT DE RECHERCHE**		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non
9 **RÉDUCTION DU TAUX DES REDEVANCES**		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :*
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 **SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)**

GILLES KREMER
PRESIDENT
MAGIC AXESS SA

VISA DE LA PRÉFECTURE

A. PAGNIER

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
DSL 1 à 7		8 à 11		30/4/01	14 MAI 2001 - B B
[redacted] 1					

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifées).

La présente invention concerne un procédé et un dispositif de certification. En particulier, la présente invention concerne la transmission de données en ligne, par exemple sur le réseau Internet.

Du fait de sa nature ouverte, Internet a augmenter les besoins de sécurité de transmission de données. En effet, l'architecture même de l'Internet le rend particulièrement vulnérable : le protocole IP; totalement décentralisé, fait circuler les datagrammes, ou "paquets" sans qu'ils soient protégés. Les adresses IP elles-mêmes, gérées par les DNS (Domain Name Servers pour serveurs de noms de domaines), ne sont pas à l'abri d'actions de malveillance. Les systèmes d'exploitation ont des failles de sécurité. D'où une liste impressionnante de menaces :

- écoute de paquets ou "sniffing";
- substitution de paquets ou "spoofing";
- piratage de DNS;
- déni de service;
- intrusions; et
- dissémination de programmes malveillants, virus et chevaux de Troie.

La cryptologie n'a pas réponse à toutes ces questions. En cryptologie, une clé est insérée au moment du chiffrement des données afin d'assurer la confidentialité de celles-ci. Les différentes normes de sécurité disponibles, pour le courrier électronique, pour les sessions de communication du web (SSL ou Secure Socket Layer pour couche de sécurité), pour le protocole IP lui-même (IPsec), mettent en oeuvre tout l'arsenal des méthodes modernes : authentification et signature, échange de clé conventionnelle, chiffrement symétrique. Des centaines de millions de clés RSA ont ainsi été produites.

Il se pose alors de nouveaux problèmes : comment gérer ces clés ? Comme le souligne un article paru dans le monde , signé par monsieur Jacques Stern du 12

septembre 2000 intitulé : "la cryptographie à l'ère de l'informatique", "il est illusoire d'utiliser un chiffrement RSA en laissant traîner ses clés secrètes sur un disque dur mal protégé contre les intrusions". En outre se pose la question de lier une clé publique RSA à son propriétaire légitime.

La présente invention entend remédier à tout ou partie de ces inconvénients. A cet effet, la présente invention vise, selon un premier aspect, un procédé de certification, caractérisé en ce qu'il comporte :

- une opération de réception d'un certificat jetable;
- une opération de chiffrement de données avec ledit certificat jetable;
- une opération de transmission des données chiffrées;
- une opération de signature de la transmission desdites données; et
- une opération de révocation dudit certificat jetable.

Selon un deuxième aspect, la présente invention vise un procédé de certification, caractérisé en ce qu'il comporte :

- une première opération de signature de données par un dispositif de fourniture desdites données sans clé privée de l'utilisateur qui fournit lesdites données; et
- une deuxième opération de signature de données qui substitue à la première signature, une deuxième signature mettant en oeuvre une clé privée dudit utilisateur.

Selon un troisième aspect, la présente invention vise un procédé de transmission de données, caractérisé en ce qu'il comporte :

- une opération de transmission desdites données d'un premier système informatique à un deuxième système informatique;
- une opération de génération d'une clé représentative desdites données, à partir desdites données;
- une opération de transmission de ladite clé par ledit deuxième système informatique;
- une opération d'authentification de l'émetteur desdites données mettant en oeuvre ladite clé; et
- une opération de vérification de ladite clé.

Grâce à chacun de ces aspects, les clés ou certificats ne sont pas stockés sur un terminal utilisateur, ce qui les protège contre tout risque de vol ou de copie. En outre, la certification peut ainsi être indépendante du terminal mis en oeuvre par le signataire, ce qui rend la signature portable d'un système à un autre.

D'autres avantages, buts et caractéristiques de la présente invention ressortiront de la description qui va suivre faite en regard du dessin annexé dans lequel la figure 1 représente une succession d'opérations effectuées par des terminaux utilisateurs et un serveur de certification, dans un mode de réalisation particulier de la présente invention.

En figure 1 sont représentés un poste utilisateur 100, une application Internet 110, une salle blanche 120, une mémoire de stockage 130, un deuxième réseau de communication 140 et un récepteur 150 sur le deuxième réseau. La salle blanche 120 comporte une protection firewall 160, un serveur de sécurité 170 et un générateur de certificats 180. Les opérations effectuées dans le mode de réalisation particulier illustré en figure 1 sont représentées dans des rectangles et numérotées de 1 à 11.

Le poste utilisateur 100 est, par exemple, un ordinateur personnel (PC) ou un ordinateur de réseau (NC). Le poste utilisateur 100 est doté d'un logiciel de communication à distance pour mettre en oeuvre l'application Internet 110, conjointement avec le serveur de sécurité 170. Ce logiciel de communication à distance peut être un logiciel de navigation ou un logiciel de courrier électronique, par exemple.

L'application Internet 110 permet la communication entre le poste utilisateur 100 et le serveur de sécurité 170 et la transmission de données depuis le poste utilisateur 100 vers la mémoire de stockage 130, par exemple par l'intermédiaire du serveur de sécurité 170. La salle blanche 120 est un espace protégé contre toute intrusion physique; tel qu'une salle de coffre d'une banque. La mémoire de stockage 130 est une mémoire adaptée à conserver des données pendant une longue période, qui dépasse une année.

Le deuxième réseau de communication 140 est, par exemple, un réseau téléphonique et, encore plus particulièrement un réseau de téléphonie mobile ou de récepteurs alphanumériques communément appelés "pageurs". Le deuxième réseau 140 est appelé "deuxième" par comparaison avec le réseau Internet, que l'on nomme aussi "premier" réseau dans la suite de la présente demande de brevet. Le deuxième réseau 140 est adapté à transmettre une clé ou certificat depuis le serveur de sécurité 170 jusqu'au récepteur 150. Le récepteur 150 sur le deuxième réseau 140 peut, selon le type de deuxième réseau 140, être un téléphone mobile, un pageur ou un récepteur quelconque. Le récepteur 150 permet à l'utilisateur du poste utilisateur 100 de prendre connaissance d'informations transmises par le serveur de sécurité 170.

La protection firewall 160 est de type logicielle et interdit toute intrusion logicielle dans le serveur de sécurité 170. Le serveur de sécurité 170 est un serveur informatique de type connu. Enfin, le générateur de certificats 180 est adapté à générer des certificats jetables, par exemple de type conforme à la norme X509-V3.

Le poste utilisateur 100 et le serveur de sécurité 170 sont conjointement adaptés à mettre en oeuvre les opérations indiquées ci-dessous. Par exemple, le serveur de sécurité 170 est adapté à fournir des routines applicatives ou "applets" au poste utilisateur 100.

Au début du processus de certification, on suppose que des données sont à transmettre de manière certifiée et signée depuis le poste utilisateur 100 jusqu'à la mémoire de stockage 130. L'utilisateur du poste utilisateur 100 se connecte au serveur de sécurité 120 pour lancer le processus de certification.

Au cours de l'opération 1, l'application Internet 110 télécharge une routine applicative certifiée dans le poste utilisateur 100. On observe que la routine applicative en question peut n'être téléchargée que dans le cas où une copie de cette routine n'est ps déjà implantée dans le poste utilisateur 100. Cette caractéristique particulière permet de rendre portable le procédé de certification objet de la présente invention, sans ralentir ce processus dans le cas où l'utilisateur met successivement en oeuvre le même poste utilisateur 100, pour plusieurs certifications de données. Au cours de l'opération 2, le générateur de certificats 180 génère un certificat jetable, par exemple sous la forme d'une clé privée conforme à la norme X509-V3. Par exemple, le certificat jetable est généré aléatoirement par le générateur 180.

Au cours de l'opération 3, le serveur de sécurité 170 transmet le certificat jetable au poste utilisateur 100. Au cours de l'opération 4, le poste utilisateur, et en oeuvre la routine applicative téléchargée au cours de l'opération 1 pour obtenir une trace des données à transmettre, appelé "hash", trace qui dépend du certificat jetable généré au cours de l'opération 2 et qui permet la détection de toute modification ultérieure des données à transmettre.

Au cours de l'opération 5, les données à transmettre et la trace ou hash sont téléchargés depuis le poste utilisateur 100 jusqu'à l'application Internet 110. Au cours de l'opération 6, l'intégrité des données à transmettre est vérifiée, en mettant en oeuvre la clé jetable générée au cours de l'opération 2 et la trace ou hash.

On observe qu'à la fin de l'opération 6, une copie des données à transmettre à été faite depuis le poste utilisateur 100 dans l'application Internet 110 et que cette copie

est certifiée conforme à l'original grâce à la mise en oeuvre d'une clé jetable. Pour éviter que le certificat jetable soit réutilisé, au cours de l'opération 10, le certificat jetable est révoqué, c'est-à-dire qu'il devient inutilisable pour certifier des données.

Les opérations 7 et 8 correspondent à un exemple de signature pouvant être utilisé en combinaison avec les opérations 1 à 6 ci-dessus. Au cours de l'opération 7, un sceau secret est généré et transmis, par l'intermédiaire du deuxième réseau 140, au récepteur 150 Par exemple, le sceau secret est tiré aléatoirement. Selon des variantes, le sceau secret dépend des données à transmettre, de leur nombre, de leur contenu, de la date et de l'heure de la génération du sceau, et/ou d'un numéro de la session Internet au cours de laquelle les données sont transmises. Le lecteur pourra se référer à la demande de brevet PCT/FR98/02348 pour mieux connaître des exemples d'étapes mises en oeuvre au cours des opérations 7 et 8. Au cours de l'opération 8, l'utilisateur commun du poste utilisateur 100 et du récepteur 150 saisie le sceau secret et celui-ci est transmis à l'application Internet 110 où le sceau est vérifié.

A la fin de l'opération 8, les données transmises sont donc certifiées intègres et signées par l'utilisateur qui les transmet. L'opération 9 consiste à substituer une signature dite PKI (pour Public Key Infrastructure, soit infrastructure de clés publiques) à la signature effectuée au cours des opérations 7 et 8.

Au cours de l'opération 9, les données transmises sont signées avec la clé privée de l'utilisateur qui les a transmise (dit "signataire" des données).

Enfin, au cours de l'opération 11, les données transmises, certifiées et signées par clé privée sont transmises à la mémoire de stockage 130 avec une date de telle manière qu'elles sont horodatées, archivées et notarisée.

Dans une application de la présente invention à une remise en main propre des données transmises, un destinataire est, à la suite de l'opération 11, averti de la mise à sa disposition des données à transmettre et des opérations similaires aux opérations exposées ci-dessus sont mises en oeuvre pour effectuer une copie certifiée conforme sur le poste utilisateur du destinataire après avoir recueilli de sa part une signature. Par exemple, une signature telle qu'exposée dans la demande de brevet PCT/FR98/02348 peut, de nouveau être mise en oeuvre pour authentifier le destinataire.

REVENDICATIONS

1. Procédé de certification, caractérisé en ce qu'il comporte :

- une opération de génération d'un certificat jetable (2);
- une opération de réception d'un certificat jetable (3);
- une opération de chiffrement de données avec ledit certificat jetable (4);
- une opération de transmission des données chiffrées (5);
- une opération de signature de la transmission desdites données (7-8); et
- une opération de révocation dudit certificat jetable (10).

2. Procédé de certification selon la revendication 1, caractérisé en ce que, au cours de l'opération de génération de certificat jetable, une clé privée est générée.

3. Procédé de certification selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que, au cours de l'opération de chiffrement, une trace des données à transmettre est déterminée sous la forme connue sous le nom de "hash".

4. Procédé de certification selon l'une quelconque des revendications 1 à 3, caractérisé en ce que, au cours de l'opération de chiffrement, est mise en oeuvre un routine applicative préliminairement téléchargée.

5. Procédé de certification selon l'une quelconque des revendications 1 à 4, caractérisé en ce que, au cours de l'opération de transmission des données chiffrées, les données à transmettre sont aussi transmises.

6. Procédé de certification selon l'une quelconque des revendications 1 à 5, caractérisé en ce que, au cours de l'opération de signature, un sceau secret est transmis à un récepteur (150) sur un réseau de télécommunication et saisi par le signataire sur un poste utilisateur qui a transmis les données à transmettre.

7. Procédé de certification selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il comporte une opération de substitution de signature au cours de laquelle une clé privée du signataire est associée aux données à transmettre.

8. Procédé de certification selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comporte une opération d'association d'une date et d'une heure aux données transmises.

9. Procédé de certification selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il comporte une opération de mise en mémoire des données transmises et d'une signature.

10. Dispositif de certification, caractérisé en ce qu'il comporte :

- un moyen de génération d'un certificat jetable;
- un moyen de réception d'un certificat jetable;
- un moyen de chiffrement de données avec ledit certificat jetable;
- un moyen de transmission des données chiffrees;
- un moyen de signature de la transmission desdites données; et
- un moyen de révocation dudit certificat jetable.

PROCEDE ET DISPOSITIF DE CERTIFICATION

La présente invention concerne un procédé et un dispositif de certification. En particulier, la présente invention concerne la transmission de données en ligne, par exemple sur le réseau Internet.

Du fait de sa nature ouverte, Internet a augmenter les besoins de sécurité de transmission de données. En effet, l'architecture même de l'Internet le rend particulièrement vulnérable : le protocole IP; totalement décentralisé, fait circuler les datagrammes, ou "paquets" sans qu'ils soient protégés. Les adresses IP elles-mêmes, gérées par les DNS (Domain Name Servers pour serveurs de noms de domaines), ne sont pas à l'abri d'actions de malveillance. Les systèmes d'exploitation ont des failles de sécurité. D'où une liste impressionnante de menaces :

- écoute de paquets ou "sniffing";
- substitution de paquets ou "spoofing";
- piratage de DNS;
- déni de service;
- intrusions; et
- dissémination de programmes malveillants, virus et chevaux de Troie.

La cryptologie n'a pas réponse à toutes ces questions. En cryptologie, une clé est insérée au moment du chiffrement des données afin d'assurer la confidentialité de celles-ci. Les différentes normes de sécurité disponibles, pour le courrier électronique, pour les sessions de communication du web (SSL ou Secure Socket Layer pour couche de sécurité), pour le protocole IP lui-même (IPsec),

mettent en oeuvre tout l'arsenal des méthodes modernes : authentification et signature, échange de clé conventionnelle, chiffrement symétrique. Des centaines de millions de clés RSA ont ainsi été produites.

Il se pose alors de nouveaux problèmes : comment gérer ces clés ? Comme le souligne un article paru dans le monde, signé par monsieur Jacques Stern du 12 septembre 2000 intitulé : la cryptographie à l'ère de l'informatique, "il est illusoire d'utiliser un chiffrement RSA en laissant traîner ses clés secrètes sur un disque dur mal protégé contre les intrusions". En outre se pose la question de lier une clé publique RSA à son propriétaire légitime.

La présente invention entend remédier à tout ou partie de ces inconvénients. A cet effet, la présente invention vise, selon un premier aspect, un procédé de certification, caractérisé en ce qu'il comporte :

- une opération de réception d'un certificat jetable;
- une opération de chiffrement de données avec ledit certificat jetable;
- une opération de transmission des données chiffrées;
- une opération de signature de la transmission desdites données; et
- une opération de révocation dudit certificat jetable.

Selon un deuxième aspect, la présente invention vise un procédé de certification, caractérisé en ce qu'il comporte :

- une première opération de signature de données par un dispositif de fourniture

desdites données sans clé privée de l'utilisateur qui fournit lesdites données; et

- une deuxième opération de signature de données qui substitue à la première signature, une deuxième signature mettant en oeuvre une clé privée dudit utilisateur.

Selon un troisième aspect, la présente invention vise un procédé de transmission de données, caractérisé en ce qu'il comporte :

- une opération de transmission desdites données d'un premier système informatique à un deuxième système informatique;
- une opération de génération d'une clé représentative desdites données, à partir desdites données;
- une opération de transmission de ladite clé par ledit deuxième système informatique;
- une opération d'authentification de l'émetteur desdites données mettant en oeuvre ladite clé; et
- une opération de vérification de ladite clé.

Grâce à chacun de ces aspects, les clés ou certificats ne sont pas stockés sur un terminal utilisateur, ce qui les protège contre tout risque de vol ou de copie. En outre, la certification peut ainsi être indépendante du terminal mis en oeuvre par le signataire, ce qui rend la signature portable d'un système à un autre.

D'autres avantages, buts et caractéristiques de la présente invention ressortiront de la description qui va suivre faite en regard du dessin annexé dans lequel la figure 1 représente une succession

d'opérations effectuées par des terminaux utilisateurs et un serveur de certification, dans un mode de réalisation particulier de la présente invention.

En figure 1 sont représentés un poste utilisateur 100, une application Internet 110, une salle blanche 120, une mémoire de stockage 130, un deuxième réseau de communication 140 et un récepteur 150 sur le deuxième réseau. La salle blanche 120 comporte une protection firewall 160, un serveur de sécurité 170 et un générateur de certificats 180. Les opérations effectuées dans le mode de réalisation particulier illustré en figure 1 sont représentées dans des rectangles et numérotées de 1 à 11.

Le poste utilisateur 100 est, par exemple, un ordinateur personnel (PC), ou un ordinateur de réseau (NC). Le poste utilisateur 100 est doté d'un logiciel de communication à distance pour mettre en oeuvre l'application Internet 110, conjointement avec le serveur de sécurité 170. Ce logiciel de communication à distance peut être un logiciel de navigation ou un logiciel de courrier électronique, par exemple.

L'application Internet 110 permet la communication entre le poste utilisateur 100 et le serveur de sécurité 170 et la transmission de données depuis le poste utilisateur 100 vers la mémoire de stockage 130, par exemple par l'intermédiaire du serveur de sécurité 170. La salle blanche 120 est un espace protégé contre toute intrusion physique ; telle qu'une salle de coffre d'une banque. La mémoire de stockage 130 est une mémoire adaptée à conserver des données pendant une longue période, qui dépasse une année.

Le deuxième réseau de communication 140 est, par exemple, un réseau téléphonique et, encore plus particulièrement un réseau de téléphonie mobile ou de récepteurs alphanumériques communément appelés "pageurs". Le deuxième réseau 140 est appelé "deuxième" par comparaison avec le réseau Internet, que l'on nomme aussi "premier" réseau dans la suite de la présente demande de brevet. Le deuxième réseau 140 est adapté à transmettre une clé ou certificat depuis le serveur de sécurité 170 jusqu'au récepteur 150. Le récepteur 150 sur le deuxième réseau 140 peut, selon le type de deuxième réseau 140, être un téléphone mobile, un pageur ou un récepteur quelconque. Le récepteur 150 permet à l'utilisateur du poste utilisateur 100 de prendre connaissance d'informations transmises par le serveur de sécurité 170.

La protection firewall 160 est de type logicielle et interdit toute intrusion logicielle dans le serveur de sécurité 170. Le serveur de sécurité 170 est un serveur informatique de type connu. Enfin, le générateur de certificats 180 est adapté à générer des certificats jetables, par exemple de type conforme à la norme X509-V3.

Le poste utilisateur 100 et le serveur de sécurité 170 sont conjointement adaptés à mettre en oeuvre les opérations indiquées ci-dessous. Par exemple, le serveur de sécurité 170 est adapté à fournir des routines applicatives ou "applets" au poste utilisateur 100.

Au début du processus de certification, on suppose que des données sont à transmettre de manière certifiée et signée depuis le poste utilisateur 100

jusqu'à la mémoire de stockage 130. L'utilisateur du poste utilisateur 100 se connecte au serveur de sécurité 120 pour lancer le processus de certification.

Au cours de l'opération 1, l'application Internet 110 télécharge une routine applicative certifiée dans le poste utilisateur 100. On observe que la routine applicative en question peut n'être téléchargée que dans le cas où une copie de cette routine n'est pas déjà implantée dans le poste utilisateur 100. Cette caractéristique particulière permet de rendre portable le procédé de certification objet de la présente invention, sans ralentir ce processus dans le cas où l'utilisateur met successivement en oeuvre le même poste utilisateur 100, pour plusieurs certifications de données. Au cours de l'opération 2, le générateur de certificats 180 génère un certificat jetable, par exemple sous la forme d'une clé privée conforme à la norme X509-V3. Par exemple, le certificat jetable est généré aléatoirement par le générateur 180.

Au cours de l'opération 3, le serveur de sécurité 170 transmet le certificat jetable au poste utilisateur 100. Au cours de l'opération 4, le poste utilisateur, et en oeuvre la routine applicative téléchargée au cours de l'opération 1 pour obtenir une trace des données à transmettre, appelé « hash », trace qui dépend du certificat jetable généré au cours de l'opération 2 et qui permet la détection de toute modification ultérieure des données à transmettre.

Au cours de l'opération 5, les données à transmettre et la trace ou hash sont téléchargés

Feuille rectifiée

depuis le poste utilisateur 100 jusqu'à l'application Internet 110. Au cours de l'opération 6, l'intégrité des données à transmettre est vérifiée, en mettant en oeuvre la clé jetable générée au cours de l'opération 2 et la trace ou hash.

On observe qu'à la fin de l'opération 6, une copie des données à transmettre à été faite depuis le poste utilisateur 100 dans l'application Internet 110 et que cette copie est certifiée conforme à l'original grâce à la mise en oeuvre d'une clé jetable. Pour éviter que le certificat jetable soit réutilisé, au cours de l'opération 10, le certificat jetable est révoqué, c'est-à-dire qu'il devient inutilisable pour certifier des données.

Les opérations 7 et 8 correspondent à un exemple de signature pouvant être utilisé en combinaison avec les opérations 1 à 6 ci-dessus. Au cours de l'opération 7, un sceau secret est généré et transmis, par l'intermédiaire du deuxième réseau 140, au récepteur 150. Par exemple, le sceau secret est tiré aléatoirement. Selon des variantes, le sceau secret dépend des données à transmettre, de leur nombre, de leur contenu, de la date et de l'heure de la génération du sceau, et/ou d'un numéro de la session Internet au cours de laquelle les données sont transmises. Le lecteur pourra se référer à la demande de brevet PCT/FR98/02348 pour mieux connaître des exemples d'étapes mises en oeuvre au cours des opérations 7 et 8. Au cours de l'opération 8, l'utilisateur commun du poste utilisateur 100 et du récepteur 150 saisie le sceau secret et celui-ci est transmis à l'application Internet 110 où le sceau est vérifié.

A la fin de l'opération 8, les données transmises sont donc certifiées intègres et signées par l'utilisateur qui les transmet. L'opération 9 consiste à substituer une signature dite PKI (pour Public Key Infrastructure, soit infrastructure de clés publiques) à la signature effectuée au cours des opérations 7 et 8.

Au cours de l'opération 9, les données transmises sont signées avec la clé privée de l'utilisateur qui les a transmise (dit "signataire" des données).

Enfin, au cours de l'opération 11, les données transmises, certifiées et signées par clé privée sont transmises à la mémoire de stockage 130 avec une date de telle manière qu'elles sont horodatées, archivées et notarisées.

Dans une application de la présente invention à une remise en main propre des données transmises, un destinataire est, à la suite de l'opération 11, averti de la mise à sa disposition des données à transmettre et des opérations similaires aux opérations exposées ci-dessus sont mises en oeuvre pour effectuer une copie certifiée conforme sur le poste utilisateur du destinataire après avoir recueilli de sa part une signature. Par exemple, une signature telle qu'exposée dans la demande de brevet PCT/FR98/02348 peut, de nouveau être mise en oeuvre pour authentifier le destinataire.

REVENDICATIONS

1. Procédé de certification, caractérisé en ce qu'il comporte :

- une opération de génération d'un certificat jetable (2);
- une opération de réception d'un certificat jetable (3);
- une opération de chiffrement de données avec ledit certificat jetable (4);
- une opération de transmission des données chiffrées (5);
- une opération de signature de la transmission desdites données (7-8); et
- une opération de révocation dudit certificat jetable (10).

2. Procédé de certification selon la revendication 1, caractérisé en ce que, au cours de l'opération de génération de certificat jetable, une clé privée est générée.

3. Procédé de certification selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que, au cours de l'opération de chiffrement, une trace des données à transmettre est déterminée sous la forme connue sous le nom de « hash ».

4. Procédé de certification selon l'une quelconque des revendications 1 à 3, caractérisé en ce que, au cours de l'opération de chiffrement, est mise en oeuvre un routine applicative préliminairement téléchargée.

5. Procédé de certification selon l'une quelconque des revendications 1 à 4, caractérisé en ce que, au cours de l'opération de transmission des

données chiffrées, les données à transmettre sont aussi transmises.

6. Procédé de certification selon l'une quelconque des revendications 1 à 5, caractérisé en ce que, au cours de l'opération de signature, un sceau secret est transmis à un récepteur (150) sur un réseau de télécommunication et saisi par le signataire sur un poste utilisateur qui a transmis les données à transmettre.

7. Procédé de certification selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il comporte une opération de substitution de signature au cours de laquelle une clé privée du signataire est associée aux données à transmettre.

8. Procédé de certification selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il comporte une opération d'association d'une date et d'une heure aux données transmises.

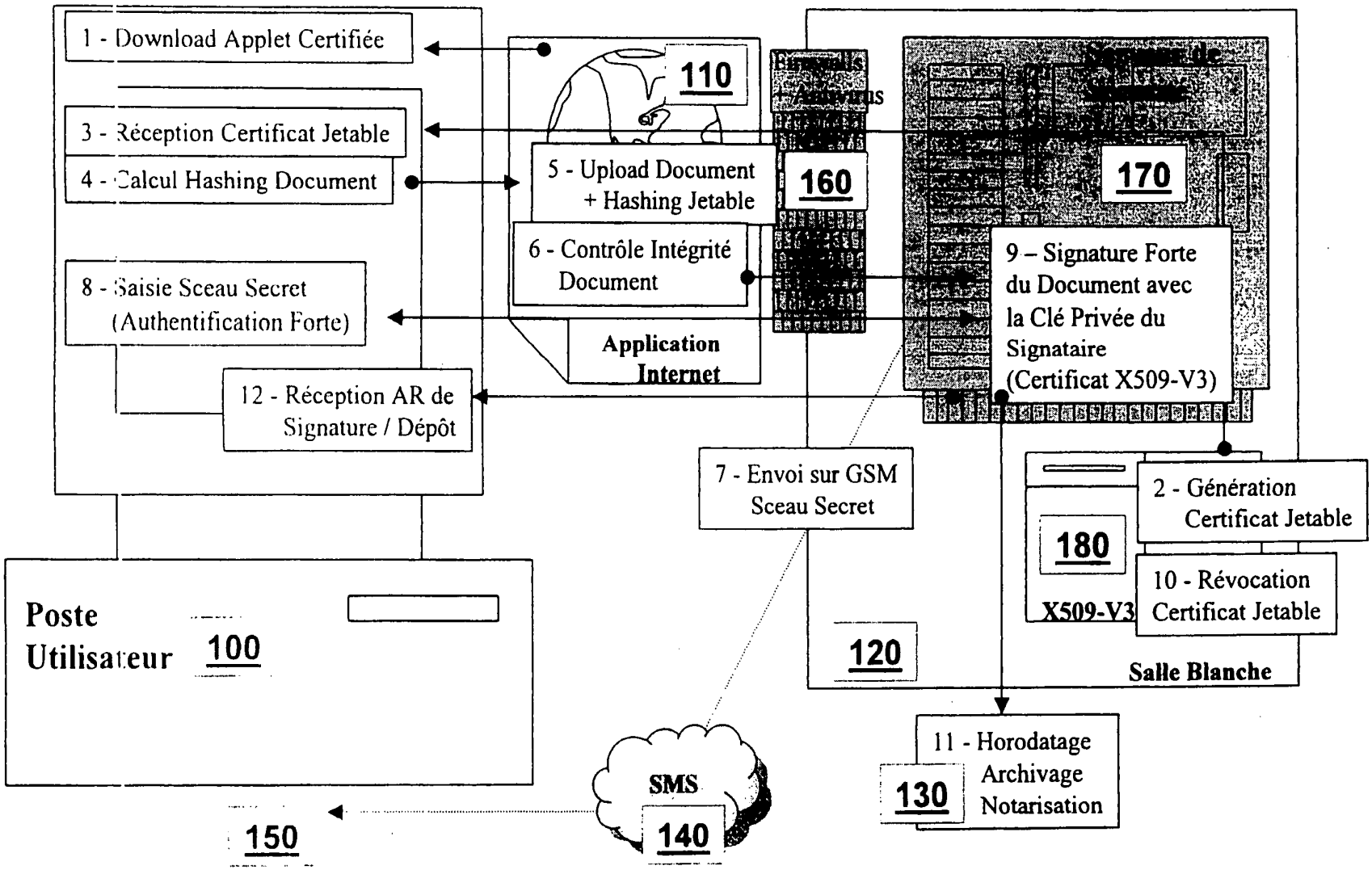
9. Procédé de certification selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il comporte une opération de mise en mémoire des données transmises et d'une signature.

10. Dispositif de certification, caractérisé en ce qu'il comporte :

- un moyen de génération d'un certificat jetable;
- un moyen de réception d'un certificat jetable;
- un moyen de chiffrement de données avec ledit certificat jetable;
- un moyen de transmission des données chiffrées;

- un moyen de signature de la transmission desdites données; et
- un moyen de révocation dudit certificat jetable.

FIGURE 1


1 - Download Applet Certifiée
3 - Réception Certificat Jetable
4 - Calcul Hashing Document
8 - Saisie Sceau Secret (Authentification Forte)
12 - Réception AR de Signature / Dépôt
110
5 - Upload Document + Hashing Jetable
6 - Contrôle Intégrité Document
Application Internet
160
170
9 – Signature Forte du Document avec la Clé Privée du Signataire (Certificat X509-V3)
7 - Envoi sur GSM Sceau Secret
2 - Génération Certificat Jetable
180
X509-V3
10 - Révocation Certificat Jetable
120
Salle Blanche
11 - Horodatage Archivage Notarisation
130
Poste Utilisateur 100
SMS
140
150